BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images may include (but are not limited to):

- BLACK BORDERS
- TEXT CUT OFF AT TOP, BOTTOM OR SIDES
- FADED TEXT
- ILLEGIBLE TEXT
- SKEWED/SLANTED IMAGES
- COLORED PHOTOS
- BLACK OR VERY BLACK AND WHITE DARK PHOTOS
- GRAY SCALE DOCUMENTS

IMAGES ARE BEST AVAILABLE COPY.

As rescanning documents *will not* correct images, please do not report the images to the Image Problem Mailbox.

DERWENT-ACC-NO: 2001-613885
DERWENT-WEEK: 200171

TITLE: Electronic commercial transaction system for internet, publishes electronic check, which guarantees payment of designated money depending on orders demand, to settle electronic transaction in orderer's side

PATENT-ASSIGNEE: SONY CORP[SONY]

PRIORITY-DATA: 2000JP-0052193 (February 23, 2000)

PATENT-FAMILY:

PUB-NO	PUB-DATE	LANGUAGE	PAGES	MAIN-IPC
JP 2001236435 A	August 31, 2001	N/A	013	G06F 017/60

APPLICATION-DATA:

PUB-NO	APPL-DESCRIPTOR	APPL-NO	APPL-DATE
JP2001236435A	N/A	2000JP-0052193	February 23, 2000

INT-CL (IPC): G06F017/60; G07F017/40 ; G09C001/00 ; H04L009/32

ABSTRACTED-PUB-NO: JP2001236435A

BASIC-ABSTRACT: NOVELTY - An electronic check issue unit publishers an electronic check which guarantees the payment of designated money depending on the demand of the orderer. The published check settles the electronic commercial transaction in the orderer's side.

DETAILED DESCRIPTION - INDEPENDENT CLAIMS are also included for the following:

(a) Electronic commercial transaction method;

(b) Information processor

USE - For electronic commercial transaction using credit card, electronic check
for networks such as internet.

ADVANTAGE - The system protects the purchaser's privacy and prevents leakage of
information about purchaser. Also safety of electronic commercial transaction
is improved reliably.

DESCRIPTION OF DRAWING(S) - The figure shows the diagram of electronic
commercial transaction system. (Drawing includes non-English language text).

CHOSEN-DRAWING: Dwg.3/5

TITLE-TERMS:
ELECTRONIC COMMERCIAL TRANSACTION SYSTEM ELECTRONIC CHECK GUARANTEE PAY
DESIGNATED MONEY DEPEND ORDER DEMAND SETTLE ELECTRONIC TRANSACTION SIDE

DERWENT-CLASS: P85 T01 T05

EPI-CODES: T01-J05A1; T05-L02;

SECONDARY-ACC-NO:
Non-CPI Secondary Accession Numbers: N2001-458262

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2001－236435
（P2001－236435A）
(43)公開日　平成13年８月31日(2001.8.31)

(51)Int.Cl.'	識別記号	FI		テーマコード'（参考）
G06F 17/60	310	G06F 17/60	310Z	5B049
	ZEC		ZEC	5B055
	410		410E	5J104
	414		414	9A001
G07F 17/40		G07F 17/40		

審査請求　未請求　請求項の数14　ＯＬ　（全 13 頁）　最終頁に続く

(21)出願番号　特願2000－52193(P2000－52193)

(22)出願日　平成12年２月23日(2000.2.23)

(71)出願人　000002185
ソニー株式会社
東京都品川区北品川６丁目７番35号
(72)発明者　船橋　武
東京都品川区北品川６丁目７番35号ソニー株式会社内
(72)発明者　塚村　善弘
東京都品川区北品川４丁目１番１号マスターエンジニアリング株式会社内
(74)代理人　100082740
弁理士　田辺　恵基

最終頁に続く

(54)【発明の名称】　電子商取引システム、電子商取引方法及び情報処理装置

(57)【要約】
【課題】電子商取引の安全性を向上させながら購入者のプライバシを保護し得る電子商取引システム、電子商取引方法及び情報処理装置を提案する。
【解決手段】電子商取引システム及び方法において、電子商取引における発注者側の要求に応じて、指定された金額の支払いを保証した電子小切手を発行し、発注者側が当該電子小切手を用いて電子商取引の決済を行うようにした。また情報処理装置において、電子商取引における発注者側の要求に応じて、指定された金額の支払いを保証した電子小切手を発行する電子小切手発行手段を設けるようにした。

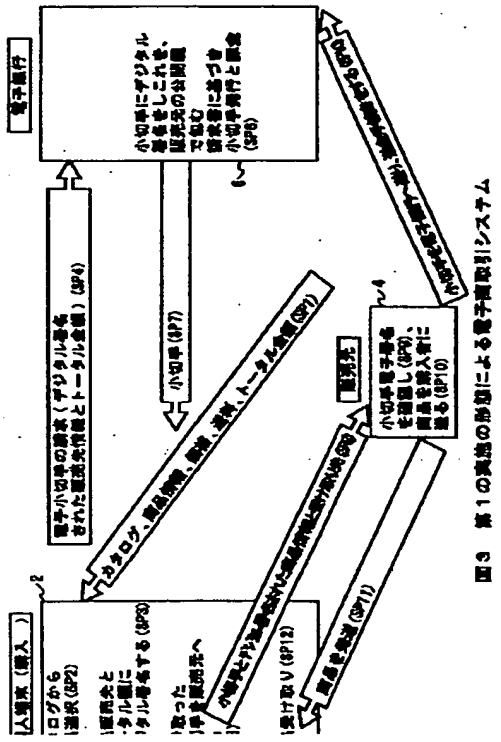

図3　第１の実施の形態による電子商取引システム

1

【特許請求の範囲】
【請求項１】電子商取引における発注者側の要求に応じて、指定された金額の支払いを保証した電子小切手を発行する電子小切手発行手段を具え、
上記発注者側は、上記電子小切手を用いて上記電子商取引の決済を行うことを特徴とする電子商取引システム。
【請求項２】上記電子小切手発行手段は、
予め上記発注者側から預かった金額の中から上記指定された金額のみを上記電子小切手に付与した識別情報と対応付けて別途管理し、
上記電子商取引の受注者側から上記電子小切手と共に与えられる支払い要求に応じて、別途管理した上記金額を上記受注者側に支払うことを特徴とする請求項１に記載の電子商取引システム。
【請求項３】上記電子小切手発行手段は、
上記発注者の身体的特徴に基づいて本人を認証した場合にのみ上記電子小切手を発行することを特徴とする請求項１に記載の電子商取引システム。
【請求項４】上記身体的特徴は、指紋であることを特徴とする請求項３に記載の電子商取引システム。
【請求項５】街頭に設置された端末装置を具え、
上記発注者側は、上記端末装置を用いて上記電子商取引を行い、
上記受注者側は、当該電子商取引において上記発注者側から発注された商品を上記端末装置と対応付けられた場所に発送することを特徴とする請求項１に記載の電子商取引システム。
【請求項６】電子商取引における発注者側の要求に応じて、指定された金額の支払いを保証した電子小切手を発行する第１のステップと、
上記発注者側が上記電子小切手を上記電子商取引の受注者側に送出するようにして当該電子商取引の決済を行う第２のステップとを具えることを特徴とする電子商取引方法。
【請求項７】上記第１のステップでは、上記電子小切手を発行すると共に、予め上記発注者側から預かった金額の中から上記指定された金額のみを上記電子小切手に付与した識別情報と対応付けて別途管理し、
上記第２のステップでは、上記決済後、上記受注者側から上記電子小切手と共に与えられる支払い要求に応じて、別途管理した上記金額を上記受注者側に支払う第３のステップを具えることを特徴とする請求項６に記載の電子商取引方法。
【請求項８】上記第１のステップでは、
上記発注者の身体的特徴に基づいて本人を認証した場合にのみ上記電子小切手を発行することを特徴とする請求項６に記載の電子商取引方法。
【請求項９】上記身体的特徴は、指紋であることを特徴とする請求項８に記載の電子商取引方法。

2

者側は、街頭に設置された端末装置を用いて上記電子商取引を行い、
上記第２のステップでは、
上記受注者側が、当該電子商取引において上記発注者側から発注された商品を上記端末装置と対応付けられた場所に発送することを特徴とする請求項６に記載の電子商取引方法。
【請求項１１】電子商取引における発注者側の要求に応じて、指定された金額の支払いを保証した電子小切手を発行する電子小切手発行手段を具えることを特徴とする情報処理装置。
【請求項１２】上記電子小切手発行手段は、
予め上記発注者側から預かった金額の中から上記指定された金額のみを上記電子小切手に付与した識別情報と対応付けて別途管理し、
上記電子商取引の受注者側から上記電子小切手と共に与えられる支払い要求に応じて、別途管理した上記金額を上記受注者側に支払うことを特徴とする請求項１１に記載の情報処理装置。
【請求項１３】上記電子小切手発行手段は、
上記発注者の身体的特徴に基づいて本人を認証した場合にのみ上記電子小切手を発行することを特徴とする請求項１１に記載の情報処理装置。
【請求項１４】上記身体的特徴は、指紋であることを特徴とする請求項１３に記載の情報処理装置。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は電子商取引システム、電子商取引方法及び情報処理装置に関し、電子商取引で用いられる購入者の購入情報の漏洩を防止して、当該購入者のプライバシを守る電子商取引システム、電子商取引方法及び情報処理装置に適用して好適なものである。
【０００２】
【従来の技術】近年、インターネット等のネットワークを介して商取引を行う電子商取引が実用化されている。電子商取引においては、決済方法としてクレジットや、電子マネー等が用いられている。
【０００３】実際に電子商取引において、購入者が例えばクレジットを用いて決済を行う場合、商品の販売元に対して購入を希望する商品の商品名（以下、これを購入情報と呼ぶ）と、購入者本人を証明する購入者の氏名、住所、年齢、電話番号及びクレジット番号などの情報（以下、これを個人情報と呼ぶ）とをインターネットを介して通知する。
【０００４】販売元は、購入者から購入情報及び個人情報を受け取ると、個人情報に基づいて購入者本人の身元を確認した後、かかる購入情報に応じた商品を購入者に販売する。

えばクレジットで受け取る際、当該クレジットのクレジット会社に対して、クレジット番号等の個人情報や、実際に購入者が購入した購入情報を通知し、クレジット会社がこれらの情報に基づいて商取引の承認した後、クレジット会社から商品の代金を受け取る。

【0006】一方電子商取引において、購入者が電子マネーを用いて決済を行う場合、銀行で希望する金額分の電子マネーを発行してもらい、当該電子マネーと購入者の氏名、住所等の商品配達に必要な情報とをインターネットを介して販売元に送出する。そして販売元は、電子マネーを受けとると、これと引換えにかかる商品を購入者に向けて商品を配達する。

【0007】

【発明が解決しようとする課題】しかしながら電子商取引において例えばクレジットによる決済方法では、取引情報をデータとして残すため、購入者が直接取引を行った販売元と共に、当該販売元が代金を請求したクレジット会社に購入者の個人情報及び購入情報が保存される。

【0008】そのためかかる電子商取引の決済方法では、内部の人間により個人情報及び購入情報が持ち出されたり、インターネットを介して侵入されて個人情報及び購入情報が盗まれる場合、購入者が直接取引を行った販売元はもとより、第三者であるクレジット会社（又は、銀行等）からも個人情報及び購入情報が漏洩し、購入者のプライバシが十分に守られない問題があった。

【0009】これに対して電子マネーを用いた決済方法では、電子マネーがインターネット上の各ポイントでの改竄等により実際に電子マネーを現金に換金できない恐れがあるため、電子マネーを受けとった販売元がこれを安心して利用できないという問題があった。

【0010】本発明は以上の点を考慮してなされたもので、電子商取引の安全性を向上させながら購入者のプライバシを保護し得る電子商取引システム、電子商取引方法及び情報処理装置を提案しようとするものである。

【0011】

【課題を解決するための手段】かかる課題を解決するため本発明においては、電子商取引システムにおいて、電子商取引における発注者側の要求に応じて、指定された金額の支払いを保証した電子小切手を発行する電子小切手発行手段を設け、発注者側が、電子小切手を用いて電子商取引の決済を行うようにした。この結果この電子商取引システムによれば、電子商取引の受注者側が電子小切手に基づいて確実に代金を得ることができ、また電子商取引によって発注者側が何を購入したか等の購入情報が受注者側以外に漏洩するのを未然に防止することができる。

【0012】また本発明においては、電子商取引方法において、電子商取引における発注者側の要求に応じて、指定された金額の支払いを保証した電子小切手を発行する電子小切手発行手段を設け、発注者側が、電子小切手を用いて電子商取引の決済を行うようにした。この結果この電子商取引方法によれば、電子商取引の受注者側が電子小切手に基づいて確実に代金を得ることができ、また電子商取引によって発注者側が何を購入したか等の購入情報が受注者側以外に漏洩するのを未然に防止することができる。

【0013】また本発明においては、情報処理装置において、電子商取引における発注者側の要求に応じて、指定された金額の支払いを保証した電子小切手を発行する電子小切手発行手段を設けるようにした。この結果この情報処理装置によれば、電子商取引の受注者側が電子小切手に基づいて確実に代金を得ることができ、また電子商取引によって発注者側が何を購入したか等の購入情報が受注者側以外に漏洩するのを未然に防止することができる。

【0014】

【発明の実施の形態】以下図面について、本発明の一実施の形態を詳述する。

【0015】（1）第1の実施の形態

（1-1）本実施の形態による電子商取引システムの構成

図1において、1は全体として本実施の形態による電子商取引システムを示し、商品の発注を行う個人端末2と、発注を受けて商品を配送する販売元3が設置した販売元サーバ4と、電子商取引で使用する電子小切手を管理する電子銀行5が設置した銀行サーバ6とがインターネット7を介して互いに接続されている。

【0016】個人端末2は、指紋照合を行う指紋照合器（ＦＩＵ: Fingurprint Identificial Unit）8と、当該指紋照合器8を制御する通常のパーソナルコンピュータ9とから構成されている。そしてパーソナルコンピュータ9は、かかる指紋照合器8を制御したり、インターネット7を介して必要なデータの送信を行い得るようになされている。

【0017】一方、販売元サーバ4及び銀行サーバ6は、後述のような各種処理を行うWWW(World Wide Web)サーバでなり、インターネット7を介して必要なＧＵＩ(Graphical User Interface)画面を表示させるための画面データを送信したり、必要なデータを暗号化して送信したり、受信した暗号化データを復号化したりすることができるようになされている。

【0018】ここで個人端末2の指紋照合器8の具体構成を図2に示す。この図2からも明らかなように指紋照合器8は、指紋採取部10と、照合コントローラ11と、当該照合コントローラ11とバス12を介して接続されたフラッシュＲＯＭ（ReadOnly Memory）13及びＲＡＭ（Random Access Memory）14と、ＣＰＵ（Central Processing Unit ）15と、当該ＣＰＵ15とバス

ログラム用フラッシュメモリ１８と、ＲＳ２３２Ｃドライバ１９とから構成されている。

【００１９】指紋採取部１０は、ＬＥＤ(Light Emitting Diode)２０、プリズム２１、レンズ鏡筒２２、ＣＣＤ(Charge Coupled Device) ２３及びアナログ／ディジタル変換器２４から形成されており、必要時にはＬＥＤ２０からプリズム２１の一面でなる指紋採取面２１Ａに向けて光Ｌ１を発射し得るようになされている。

【００２０】この光Ｌ１は、指紋採取面２１Ａ上に載せられた指２５の表明において反射し、その反射光Ｌ２がプリズム２１及びレンズ鏡筒２２を順次介してＣＣＤ２３の受光面に入光する。そしてＣＣＤ２３は、この反射光Ｌ２を光電変換し、得られた光電変換信号Ｓ１がアナログ／ディジタル変換器２４に送出される。またアナログ／ディジタル変換器２４は、供給される光電変換信号Ｓ１をディジタル変換し、得られた指紋データＤ１を照合コントローラ１１に送出する。

【００２１】照合コントローラ１１、ＲＡＭ１４をワークメモリとして用いながら、指紋採取部１０から指紋の特徴点（以下、これをテンプレートと呼ぶ）に当たる一部分（以下、これをテンプレートデータD_Tと呼ぶ）を抽出してこれをフラッシュＲＯＭ１３に格納し、又はこの指紋データＤ１をフラッシュＲＯＭ１３に予め記録されている各テンプレートデータD_Tと照合する。

【００２２】一方、ＣＰＵ１５は、ＲＳ２３２Ｃデバイス１９を介してパーソナルコンピュータ９と接続されており、このＲＳ２３２Ｃデバイス１９を通じてパーソナルコンピュータ９との間で各種コマンドやデータを送受し得るようになされている。

【００２３】そしてＣＰＵ１５は、パーソナルコンピュータ９から与えられるコマンドに基づいて、プログラム用フラッシュメモリ１７内に格納されている各種プログラムのなかから対応するプログラムを読み出してこれをプログラム用ＲＡＭ１８に展開し、このプログラムに従って各種制御処理を実行する。

【００２４】またＣＰＵ１５は、パーソナルコンピュータ９から与えられるコマンドに基づいて、必要時には後述のようにプログラム用フラッシュメモリ１８に格納されたプログラムでなる暗号エンジン２７により各種暗号鍵を作成する。

【００２５】次にこの個人端末２の各種機能について説明する。

【００２６】まずこの個人端末２の第１の機能として、購入者の指紋を登録する指紋登録機能がある。実際上この個人端末２において、パーソナルコンピュータ９は、操作されて指紋登録モードが選択されると、当該パーソナルコンピュータ９は、指紋の登録動作に入り、「指を指紋照合器に載せて下さい」といったメッセージを表示すると共に、指紋照合器８のＣＰＵ１５に対して登録コ

【００２７】この結果指紋照合器８では、指紋採取面２１Ａに指２５が載せられると、ＣＰＵ１５の制御のもとに指紋採取部１０のＬＥＤ２０が発行して指紋が採取され、この指紋データＤ１が照合コントローラ１１に与えられる。

【００２８】また照合コントローラ１１は、供給される指紋データＤ１からテンプレートデータD_Tを生成し、これをフラッシュＲＯＭ１３に格納する。このようにしてこの個人端末２では、購入者の指紋を指紋照合器８に登録する。

【００２９】またこの個人端末２の第２の機能として、購入者の指紋を登録された指紋と照合する照合機能がある。すなわちパーソナルコンピュータ３は、指紋照合モードが選択されると、「指を指紋照合器に載せてください」といったメッセージを表示すると共に、指紋照合器８のＣＰＵ１５に対して照合コマンドを発行する。

【００３０】この結果、指紋照合器８では、指紋採取面２１Ａに指が載せられると、ＣＰＵ１５の制御のもとに指紋採取部１０を介して指紋が採取され、その指紋データＤ１が照合コントローラ１１に与えられる。

【００３１】照合コントローラ１１は、供給される指紋データＤ１と、フラッシュＲＯＭ１３に格納されているテンプレートデータD_Tとを照合し、照合結果をＣＰＵ１５を介してパーソナルコンピュータ９に送出する。このようにしてこの個人端末２は、購入者の指紋を登録された指紋と照合する。

【００３２】さらにこの個人端末２の第３の機能として、指紋登録した購入者に対する暗号鍵の作成機能がある。すなわちこの個人端末２では、指紋照合によってその購入者が登録された購入者であることを認証した直後の１回のみ、その人の暗号鍵の作成及びその登録を行うことができるようになされている。

【００３３】またこの個人端末２では、暗号鍵として、電子商取引で使用する電子小切手等を暗号化及び復号化するための一対の秘密鍵及び公開鍵（以下、これらをそれぞれ個人用秘密鍵Ｃｄ、個人用公開鍵Ｃｅと呼ぶ）を作成し、これを登録することができるようになされている。

【００３４】実際上、パーソナルコンピュータ９は、暗号鍵作成モードが選択されると、まず「指を指紋照合器に載せてください」といったメッセージを表示すると共に、指紋照合器８のＣＰＵ１５に対して照合コマンドを発行する。

【００３５】このとき指紋照合器８では、ＣＰＵ１５の制御のもとに、購入者の指紋照合が行われ照合結果がパーソナルコンピュータ９に返答される。

【００３６】またこのとき指紋照合器８では、上述した指紋照合モードと同様の照合処理によって指紋採取面２１Ａに載せられた指の指紋が予め登録された購入者のも

とにフラッシュROM13に対するアクセスを1回だけ許可する。

【0037】一方、このときパーソナルコンピュータ9では、指紋照合器8からの照合結果に基づいてその購入者が登録された購入者であることを認証できたか否かを判断し、認証できなかった場合にはこの処理を終了し、これに対して認証できた場合には暗号鍵作成登録コマンドを指紋照合器8のCPU15に発行する。

【0038】そして指紋照合器8のCPU15は、この暗号鍵作成登録コマンドが与えられると、暗号エンジン27により個人用秘密鍵Cd及び個人用公開鍵Ceを購入者の指紋データD1に基づいて作成し、これを照合コントローラ11を介してフラッシュROM13に格納する。

【0039】このようにしてこの個人端末2では、指紋登録された購入者に対して個人用秘密鍵Cd及び個人用公開鍵Ceを作成し、これらを当該購入者と対応付けて指紋照合器8内において保存する。

【0040】かかる個人端末2の第3の機能に加えて、個人端末2の第4の機能として、指紋登録した購入者に対する個人用秘密鍵Cdの使用許諾機能がある。すなわちこの個人端末2では、指紋照合によってその購入者が登録された購入者であることを認証した直後の1回のみ、その人の作成した個人用秘密鍵Cdを使用することができるようになされている。

【0041】実際上、パーソナルコンピュータ9は、鍵使用モードが選択されると、まず「指を指紋照合器に載せてください」といったメッセージを表示すると共に、指紋照合器8のCPU15に対して照合コマンドを発行する。

【0042】このとき指紋照合器8では、CPU15の制御のもとに、購入者の指紋照合が行われ照合結果がパーソナルコンピュータ9に返答される。

【0043】またこのとき指紋照合器8では、上述した指紋照合モードと同様の照合処理によって指紋採取面21Aに載せられた指の指紋が予め登録された購入者のものであると認証できた場合には、CPU15の制御のもとにフラッシュROM13に対するアクセスを1回だけ許可する。

【0044】一方、このときパーソナルコンピュータ9では、指紋照合器8からの照合結果に基づいてその購入者が登録された購入者であることを認証できたか否かを判断し、認証できなかった場合にはこの処理を終了し、これに対して認証できた場合には秘密鍵使用コマンドを指紋照合器8のCPU15に発行する。

【0045】そして指紋照合器8のCPU15は、この秘密鍵使用コマンドが与えられて初めてフラッシュROM13にアクセスし、指紋登録された購入者の個人用秘密鍵Cd及び個人用公開鍵Ceを使用することができる。

【0046】すなわち指紋照合器8では、購入者の指紋が正しく認証されて初めて、かかる個人用秘密鍵Cd及び個人用公開鍵Ceを、取引情報を個人用公開鍵Ceで暗号化する際や、購入者の認証に利用することができる。

【0047】また指紋照合器8では、作成した個人用秘密鍵Cdを当該指紋照合器8の外部に読み出すことができないようになされており、これにより個人用秘密鍵Cdが外部に漏洩し、悪意の第三者が当該個人用秘密鍵Cdを用いて購入者本人になりすますことを防止できるようになされている。

【0048】これにより電子銀行5及び販売元3側では、かかる個人用秘密鍵Cdでディジタル署名された取引情報を受け取り、この個人用秘密鍵Cdと対で作成された個人用公開鍵Ceで認証することにより、供給された取引情報が指紋登録された購入者本人によって作成されたものであることを確認できる。

【0049】従って電子銀行5側においては、個人用秘密鍵Cdが個人端末2の認証に使用される場合、個人用秘密鍵Cdと対に作成される個人用公開鍵Ceを保管しておく必要がある。また電子銀行5は、かかる個人用公開鍵Ceを電子商取引に使用するため、この個人公開鍵Ceを使用する購入者の身元を確認し、この個人公開鍵Ceを有効なものにしておく必要がある。以下電子銀行5が有効な個人用公開鍵Ceを登録する方法について説明する。

【0050】（1-2）個人用公開鍵Ceの登録方法

まず第1の登録方法としては、電子商取引を行おうとしている購入者が実際に電子銀行5に出向き、その場で購入者自身の個人用公開鍵Ceを作成し、これを当該電子銀行5に登録する方法がある。

【0051】かかる第1の登録方法では、まず購入者が持参した運転免許証等の身分証明書により電子銀行5の銀行員に身元を確認してもらい、この後当該購入者が持参した指紋照合器8を接続コード（図示せず）を介して銀行サーバ6に接続する。

【0052】次に購入者が、個人端末2の第1の機能について上述した指紋登録手順に従って自己の指紋の指紋を指紋照合器8に登録し、この後個人端末2の第3の機能について上述した個人用暗号鍵の作成手順に従って、購入者の個人用公開鍵Ce及び個人用秘密鍵Cdを指紋照合器8に作成させる。そしてこのようにして作成した個人用公開鍵Ce及び個人用秘密鍵Cdのうちの個人用公開鍵Ceのみを、指紋照合器8から読み出して銀行サーバ6内に設けられたハードディスク等の記録媒体に記録する（以下、これを銀行サーバ6に登録するという）。

【0053】かくしてこの第1の登録方法によれば、購入者の身元を確認した後に作成された個人用公開鍵Ce

において当該個人用公開鍵Ｃｅに信頼性を担保することができる。

【００５４】また第２の登録方法としては、個人端末２で作成した個人用公開鍵Ｃｅをインターネット７を介して銀行サーバ６に配送して、登録する方法がある。

【００５５】かかる第２の登録方法では、まず電子銀行５側において、購入者の個人用公開鍵Ｃｅをインターネット７を介して銀行サーバ６に配送する際の暗号鍵として、個人端末２の第３の機能について上述した個人用暗号鍵の作成手順に従って一対の鍵配送用公開鍵Ｄｅ及び鍵配送用秘密鍵Ｄｄを指紋照合器８に作成させ、これらのうち鍵配送用公開鍵Ｄｅのみを銀行サーバ６に登録する。

【００５６】そしてこの後、この指紋照合器８を、内部に鍵配送用公開鍵Ｄｅ及び鍵配送用秘密鍵Ｄｄが格納された状態のまま電子銀行５側から購入者に配達する。

【００５７】一方購入者側に置いては、配達された指紋照合器８を用い、上述の指紋登録手順に従って自己の指紋の指紋データを指紋照合器８に登録し、この後上述の個人用暗号鍵の作成手順に従って、一対の個人用公開鍵Ｃｅ及び個人用秘密鍵Ｃｄを作成させる。

【００５８】そして購入者は、この後このようにして作成した自己の個人用公開鍵Ｃｅを指紋照合器８内に予め格納されている鍵配送用秘密鍵Ｄｄで暗号化（ディジタル署名）することにより、認証用の署名公開鍵〔（Ｃｅ）^{Dd}〕を作成し、これをインターネット７を介して電子銀行５の銀行サーバ６に送出する。

【００５９】さらに電子銀行５側では、この署名公開鍵〔（Ｃｅ）^{Dd}〕を受け取ると、これを銀行サーバ６に登録されている鍵配送用公開鍵Ｄｅで認証（復号化）する。そして電子銀行５側では、認証公開鍵〔（Ｃｅ）^{Dd}〕が正しく認証された場合には、認証（復号化）して得た個人用公開鍵Ｃｅと、かかる鍵配送用公開鍵Ｄｅとを、これらに対応する購入者の身元を保証する身元情報に対応付けて銀行サーバ６に登録する。

【００６０】かくして第２の登録方法によれば、ディジタル署名された個人用公開鍵Ｃｅをインターネット７を介して銀行サーバ６に送出することにより、電子銀行５側において確実にかかる個人用公開鍵Ｃｅを登録することができる。

【００６１】（１－３）本実施の形態による電子商取引手順

ここで図１との対応部分に同一符号を付して示す図３を用いて、電子小切手を使用して商品の購入を行うその取引状況を説明する。

【００６２】ここで電子小切手は、金額の支払いを保証し、後述のように小切手番号、合計金額及び電子銀行証明書を含んでなるデータである。

【００６３】かかる電子商取引システム１においては、は販売元の契約する電子銀行５からインターネット７を介して個人端末２に配送される（ステップＳＰ１）。

【００６４】この場合電子商品カタログは、商品名やそのその商品の説明をした商品情報、価格、送料及び販売元の販売元ＩＤ(Identification)などのデータから構成されるものである。かくして購入者は、個人端末２のパーソナルコンピュータ９のディスプレイ（図示せず）でかかる電子商品カタログを閲覧して、購入を希望する商品を選択することができる。

【００６５】そして購入者は、電子商取引を利用して商品を購入する場合には、まず以下の商品購入手続き手順に従って商品購入の準備をする。

【００６６】すなわち購入者は、まずパーソナルコンピュータ９のディスプレイに表示される電子カタログを見ながら購入を希望する商品を選択する（ステップＳＰ２）。このときパーソナルコンピュータ９は、その購入商品の合計金額を算出し、算出した結果をかかる電子カタログに表示する。

【００６７】続けて購入者は、パーソナルコンピュータ９を用いて電子銀行５に対して電子小切手の発行を依頼する所定の操作を行う。このときパーソナルコンピュータ９は、各部を制御し、指定された商品の合計金額の合計金額データ（以下、これを単に合計金額と呼ぶ）と、当該商品を扱う販売元の販売元ＩＤとを電子カタログから読み取り、当該読み取った合計金額及び販売元ＩＤのハッシュ値（Ｈ１）をハッシュ関数に基づいて算出し、算出結果を指紋照合器８に送出する。

【００６８】ここで指紋照合器８は、指紋取得部１０で取得した指紋データを正しく認証できると初めて個人用公開鍵Ｃｅ及び個人用秘密鍵Ｃｄを使用し得る状態となり、この場合に限りパーソナルコンピュータ９から供給されたハッシュ値（Ｈ１）を予め作成しておいた個人用秘密鍵Ｃｄでディジタル署名して署名情報〔（Ｈ１）^{Cd}〕を作成する（ステップＳＰ３）。そして指紋照合器８は、この後この署名情報〔（Ｈ１）^{Cd}〕をパーソナルコンピュータ９に送出する。

【００６９】因みにハッシュ関数は情報量を丸めて（圧縮して）ハッシュ値を算出する。従って指紋照合器８は、情報量が丸められた例えば合計金額及び販売元ＩＤのハッシュ値（Ｈ１）にディジタル署名することにより、もとの合計金額及び販売元ＩＤにディジタル署名する場合に比べてディジタル署名や復号化等に要する処理時間を短縮することができる。

【００７０】この結果、パーソナルコンピュータ９は、この作成した署名情報〔（Ｈ１）^{Cd}〕と、単なる手続き的な情報である合計金額及び販売元ＩＤとをまとめて電子小切手依頼書ファイル〔合計金額＋販売元ＩＤ＋署名情報（Ｈ１）^{Cd}〕（以下、これを電子小切手依頼書と呼ぶ）として電子銀行５の銀行サーバ６に送出する（ステ

【００７１】一方電子銀行５側において、個人端末２から送出された電子小切手依頼書に基づいて電子小切手を発行する場合、以下の手順に従って電子小切手を発行する。

【００７２】電子銀行５側の銀行サーバ６は、個人端末２のパーソナルコンピュータ９から電子小切手依頼書〔合計金額＋販売元ＩＤ＋署名情報（Ｈ１）^{Cd}〕が供給されると、当該供給先である購入者の個人用公開鍵Ｃｅを当該電子銀行６内の記録媒体から再生し、電子小切手依頼書〔合計金額＋販売元ＩＤ＋署名情報（Ｈ１）^{Cd}〕の署名情報〔（Ｈ１）^{Cd}〕を個人用公開鍵Ｃｅで認証（復号化）する。

【００７３】続けて銀行サーバ６は、かかる認証が正しく行われた場合、電子小切手依頼書〔合計金額＋販売元ＩＤ＋署名情報（Ｈ１）^{Cd}〕のもとの合計金額及び販売元ＩＤのハッシュ値（Ｈ１′）をハッシュ関数に基づいて算出し、このハッシュ値（Ｈ１′）と認証後に得たハッシュ値（Ｈ１）とが同一であるか否かを判断する。

【００７４】ここでこれら２つのハッシュ値が同一であるということは、電子小切手依頼書〔合計金額＋販売元ＩＤ＋署名情報（Ｈ１）^{Cd}〕がインターネット７上のあるポイントで改竄されなかったことを意味し、当該電子小切手依頼書〔合計金額＋販売元ＩＤ＋署名情報（Ｈ１）^{Cd}〕の正当性が保証される。

【００７５】かくしてこのとき銀行サーバ６は、電子小切手依頼書〔合計金額＋販売元ＩＤ＋署名情報（Ｈ１）^{Cd}〕に含まれる販売元ＩＤを記憶保存して電子小切手の小切手番号を作成する。次ぎに銀行サーバ６は、小切手番号と電子小切手依頼書に記載されている合計金額と電子銀行証明書とのハッシュ値（Ｈ２）をハッシュ関数に基づいて算出する。このとき銀行サーバ６は、算出したハッシュ値（Ｈ２）を予め作成しておいた銀行用暗号鍵Ｂｄでディジタル署名して署名情報〔（Ｈ２）^{Bd}〕を作成する。

【００７６】続けて銀行サーバ６は、かかる署名情報〔（Ｈ２）^{Bd}〕を販売元ＩＤに対応する販売元３の販売元用暗号鍵Ｓｅで暗号化することにより、暗号化情報〔（（Ｈ２）^{Bd}）^{Se}〕を作成して、これに小切手番号、合計金額及び電子銀行証明書を加えたものを電子小切手〔小切手番号＋合計金額＋電子銀行証明書＋（（Ｈ２）^{Bd}）^{Se}〕として発行する（ステップＳＰ５）。

【００７７】この電子銀行証明書は、電子銀行の銀行名及びその支店名や、電子銀行で作成した公開鍵を公開鍵の認証を行う認証局で承認してもらった際に発行された電子銀行ＩＤからなる。

【００７８】因みに電子小切手〔電子銀行証明書＋小切手番号＋合計金額＋（（Ｈ２）^{Bd}）^{Se}〕においては、電子銀行証明書に記載された電子銀行の銀行名及びその支店名により、当該電子小切手〔電子銀行証明書＋小切手きるようになされている。

【００７９】そして銀行サーバ６は、電子小切手が販売元用公開鍵Ｓｅで暗号化されてなるため、これを復号化できる販売元３のみが使用可能な電子小切手〔電子銀行証明書＋小切手番号＋合計金額＋（（Ｈ２）^{Bd}）^{Se}〕を作成することができる。

【００８０】また銀行サーバ６は、販売元３側と電子商取引の契約を結んだ際に、上述の購入者の個人用公開鍵Ｃｅを登録する手順と同様の手順に従って販売元用公開鍵Ｓｅを公開鍵登録部（図示せず）に登録する。

【００８１】一方銀行サーバ６は、上述のように電子小切手を発行すると、その時点で発行した電子小切手〔電子銀行証明書＋小切手番号＋合計金額＋（（Ｈ２）^{Bd}）^{Se}〕の合計金額（合計金額データ）に相当する額をかかる購入者が開設する銀行口座から引き落とす（ステップＳＰ６）。このとき銀行サーバ６は、電子小切手〔電子銀行証明書＋小切手番号＋合計金額＋（（Ｈ２）^{Bd}）^{Se}〕の小切手番号に基づいて引き落とした現金を管理すると共に、電子小切手〔電子銀行証明書＋小切手番号＋合計金額＋（（Ｈ２）^{Bd}）^{Se}〕の合計金額分の現金を既に引き落としてしているため、当該電子小切手〔電子銀行証明書＋小切手番号＋合計金額＋（（Ｈ２）^{Bd}）^{Se}〕に対して引き落とした現金と同じ価値を持たせることができる。

【００８２】そして銀行サーバ６は、電子小切手発行処理を終了し、かかる電子小切手〔電子銀行証明書＋小切手番号＋合計金額＋（（Ｈ２）^{Bd}）^{Se}〕をインターネット７を介して個人端末２に配送する（ステップＳＰ７）。

【００８３】次に個人端末２側において電子銀行３側から配送された電子小切手〔電子銀行証明書＋小切手番号＋合計金額＋（（Ｈ２）^{Bd}）^{Se}〕を用いて実際に商品を購入する場合、以下の商品購入手順に従って商品を購入する。

【００８４】すなわちパーソナルコンピュータ９は、銀行サーバ６から電子小切手〔電子銀行証明書＋小切手番号＋合計金額＋（（Ｈ２）^{Bd}）^{Se}〕を受け取ると、当該電子小切手のハッシュ値（Ｈ３）をハッシュ関数に基づいて算出し、これを指紋照合器８において、予め作成している個人用秘密鍵Ｃｄでディジタル署名して署名情報〔（Ｈ３）^{Cd}〕を作成する。

【００８５】続けてパーソナルコンピュータ９は、購入者が所定の操作により購入を希望する商品の商品名（以下、これを発注商品名と呼ぶ）や、購入した商品の届け出先である個人端末２の住所、購入者の氏名という購入に際して必要最低限の個人情報を入力すると、これらをかかる署名情報〔（Ｈ３）^{Cd}〕に加え、もとの電子小切手、発注商品名、住所、氏名及び署名情報〔（Ｈ３）^{Cd}〕をまとめた発注伝票〔電子小切手＋発注商品名

側の販売元サーバ4に配送する（ステップSP8）。

【0086】販売元3側においては、個人端末2から配送された発注伝票〔電子小切手＋発注商品名＋住所＋氏名＋（H3）^{Cd}〕に基づいて商品を配達する場合、以下に示すような複数の認証及び確認事項を無事終了した後、購入者に向けて商品の配達を行う。

【0087】すなわちまず販売元3側の販売元サーバ4は、個人端末2のパーソナルコンピュータ9から送られてきた発注伝票〔電子小切手＋発注商品名＋住所＋氏名＋（H3）^{Cd}〕を受け取ると、当該発注伝票〔電子小切手＋発注商品名＋住所＋氏名＋（H3）^{Cd}〕のうちの電子小切手〔電子銀行証明書＋小切手番号＋合計金額＋（（H2）^{Bd}）^{Se}〕の電子銀行証明書を読み取る。

【0088】次ぎに販売元サーバ4は、読み取った電子銀行証明書に記載されている電子銀行の銀行サーバ6にアクセスし、発注伝票〔電子小切手＋発注商品名＋住所＋氏名＋（H3）^{Cd}〕の作成を依頼した購入者の個人用公開鍵Ｃｅを銀行サーバ6を介して取得する。

【0089】このとき銀行サーバ6は、販売元サーバ4から購入者の個人用公開鍵Ｃｅの供給依頼を受けると、購入者から取得した個人用公開鍵Ｃｅのハッシュ値（H4）を算出し、当該算出したハッシュ値（H4）を銀行用暗号鍵Ｂｄでディジタル署名して署名情報〔（H4）^{Bd}〕を作成する。そして銀行サーバ6は、作成した署名情報〔（H4）^{Bd}〕と、もとの個人用公開鍵Ｃｅとをまとめて送出ファイル〔個人用公開鍵Ｃｅ＋（H4）^{Bd}〕として販売元サーバ4に送出する。

【0090】また販売元サーバ4は、電子銀行5側の正当性と当該電子銀行5側が送出した送出ファイル〔個人用公開鍵Ｃｅ＋（H4）^{Bd}〕の正当性とを確認するために、公開鍵を管理する認証局に問い合わせ、電子銀行証明書に記載されている電子銀行5側の銀行名又は銀行ＩＤに基づいて、かかる電子銀行5側の銀行用公開鍵Ｂｅを取得する。

【0091】そして販売元サーバ4は、銀行サーバ6から供給された送出ファイル〔個人用公開鍵Ｃｅ＋（H4）^{Bd}〕を受け取ると、署名情報〔（H4）^{Bd}〕をかかる銀行用公開鍵Ｂｅで認証する。

【0092】ここで署名情報〔（H4）^{Bd}〕が正しく認証できれば、原理的にその電子銀行5側しかディジタル署名できない署名情報〔（H4）^{Cd}〕が送られてきたことから、本当に当該電子銀行5側から送られてきたことが確認できる。また認証局から送られてきた銀行用公開鍵Ｂｅで、電子銀行5が送出した署名情報〔（H4）^{Bd}〕を正しく認証できたことにより、かかる電子銀行5の正当性を確認できる。

【0093】かくしてこのとき販売元サーバ4は、もとの個人用公開鍵Ｃｅのハッシュ値（H4′）ををハッシュ関数に基づいて算出し、このハッシュ値（H4′）とする。

【0094】ここでこれら2つのハッシュ値が同一であるということは、個人用公開鍵Ｃｅがインターネット7上のあるポイントで改竄されなかったことを意味し、当該個人用公開鍵Ｃｅの正当性が保証される。そして販売元サーバ4は、個人用公開鍵Ｃｅの正当性を確認すると、これを正規の個人用公開鍵Ｃｅとして当該販売元サーバ4の記録媒体に記録する。

【0095】販売元サーバ4は、銀行サーバ6から正規の個人用公開鍵Ｃｅを取得すると、個人端末2のパーソナルコンピュータ9から送られてきた発注伝票〔電子小切手＋発注商品名＋住所＋氏名＋（H3）^{Cd}〕のうちの署名情報〔（H3）^{Cd}〕を、かかる個人用公開鍵Ｃｅで認証する（ステップSP9）。

【0096】このとき販売元サーバ4は、発注伝票〔電子小切手＋発注商品名＋住所＋氏名＋（H3）^{Cd}〕のうち署名情報〔（H3）^{Cd}〕が正しく認証できれば、原理的にその購入者しかディジタル署名できない署名情報〔（H3）^{Cd}〕が送られてきたことから、本当に当該購入者から発注されたことを確認できる。

【0097】続けて販売元サーバ4は、もとの電子小切手のハッシュ値（H3′）をハッシュ関数に基づいて算出し、このハッシュ値（H3′）と認証後に得たハッシュ値（H3）とが同一か否かを判断する。

【0098】ここでこれら2つのハッシュ値が同一であるということは、電子小切手〔電子銀行証明書＋小切手番号＋合計金額＋（（H2）^{Bd}）^{Se}〕がインターネット7上のあるポイントで改竄されなかったことを意味し、当該電子小切手〔電子銀行証明書＋小切手番号＋合計金額＋（（H2）^{Bd}）^{Se}〕の正当性が保証される。

【0099】続けて販売元サーバ4は、電子小切手〔電子銀行証明書＋小切手番号＋合計金額＋（（H2）^{Bd}）^{Se}〕に施されている暗号化を公開鍵暗号化方式に基づいて、当該販売元サーバ4のみが登録する販売元用秘密鍵Ｓｄで復号化する。

【0100】これにより販売元サーバ4は、秘密裏に電子銀行証明書、小切手番号及び合計金額の署名情報（H2）^{Bd}を受け取ることができる。

【0101】続けて販売元サーバ4は、暗号化情報〔（H2）^{Bd}〕を、認証局から取り寄せた電子銀行5側の銀行用暗号鍵Ｂｅで認証する。

【0102】このとき暗号化情報〔（H2）^{Bd}〕が正しく認証できれば、原理的に電子銀行5側でしかディジタル署名できない署名情報〔（H3）^{Cd}〕が送られてきたことから、本当に電子小切手が電子銀行署名書で証明された電子銀行5から送られたことを確認できる。

【0103】これに加えて銀行サーバ6が購入者の身元を正式に確認したのちでしか、当該購入者に対してかかる電子小切手を作成しないことにより、電子小切手がか

で、当該購入者の例えば購入者の年齢、職業、電話番号、年収等の身元を敢えて確認することなく、身元の保証された購入者から商品の購入依頼が来たことを確認できる。すなわち販売元サーバ4は、電子小切手の有効性を確認できる。

【0104】続けて販売元サーバ4は、もとの小切手番号、合計金額及び電子銀行証明書のハッシュ値（H2′）を算出し、このハッシュ値（H2′）と認証後に得たハッシュ値（H2）とが同一か否かを判断する。

【0105】ここでこれら2つのハッシュ値が同一であるということは、電子銀行証明書、小切手番号及び合計金額がインターネット7上のあるポイントで改竄されなかったことを意味し、当該電子銀行証明書、小切手番号及び合計金額の正当性が保証される。

【0106】すなわち販売元サーバ4は、以上のように種々の確認を行った後、銀行サーバ6に対して認証済みの小切手番号のみを伝えれば、小切手番号に基づいて既に購入者が開設した口座から引き落とされている現金を確実に受け取ることができる（ステップSP10）。

【0107】因みに銀行サーバ6は、正規に営業を行う販売元3個の販売先IDに基づいて作成した電子小切手の小切手番号に基づいて料金請求されるため、安心してかかる販売元サーバ4に対して電子小切手の合計金額に応じた支払いをすることができる。

【0108】続けて販売元サーバ4は、電子銀行5個からの送金を確認した後、購入者側に向けて商品を配達する（ステップSP11）。

【0109】そして購入者は、自己の氏名と自宅の住所のみを用いて、販売元から配達された商品を自宅において受け取ることができる（ステップSP12）。

【0110】（1-4）本実施の形態の動作及び効果
以上の構成において、電子銀行5は、購入者の依頼に応じて電子小切手を発行する際、電子小切手を作成した時点で購入者の口座から現金を引き落とすと共に、当該引き落とした現金をかかる電子小切手の小切手番号を用いて管理する。

【0111】そして電子銀行5は、販売元3個から電子小切手の小切手番号に基づいて換金請求を請けると、当該小切手番号で管理する現金をかかる販売元3個が開設する口座に振り込む。

【0112】また電子銀行5は、指紋認証器で認証された購入者からの依頼に対してのみ電子小切手を発行するとともに、これに当該電子小切手の発行元を証明する証明書を添付する。そして電子銀行5は、小切手番号を含む電子小切手に所定の暗号化処理を施した後、これを電子商取引で利用する電子小切手として発行する。

【0113】従ってこの電子商取引システム1では、電子銀行5において、予め購入者の口座から引き落としておいた現金を小切手番号に基づいて販売元3個が開設すると販売元3との関係を知りえないと共に、販売元3は確実に集金することができる。これにより電子商取引において電子小切手が用いられると、販売元3個では電子小切手を安心して利用できると共に、電子銀行5個では購入者が販売元3からどの様なものを購入したかという購入情報を入手できない。

【0114】また販売元3個は、電子銀行5が予め購入者の口座から引き落としておいた現金と等価の電子小切手を用いて商品の販売を行うことにより、当該商品の販売先として購入者の氏名及び住所のみを知れば良い。これにより購入者は、販売元3個に対して商品の配達に必要最低限の個人情報を知らせるだけで良い。

【0115】以上の構成によれば、電子銀行5が購入者の口座から引き落としておいた現金を小切手番号に対応付けて管理することにより、小切手番号に基づいてのみ販売元3に支払いを行う。従って電子銀行5は、購入者と販売元3との関係が不明瞭となり、これにより購入者の購入情報を入手できない。また販売元3は、電子小切手を安心して利用できる。かくして電子商取引の安全性を高めながら、購入者の購入情報が洩れず、購入者のプライバシを守ることのできる電子商取引システムを実現できる。

【0116】（2）第2の実施の形態
（2-1）本実施の形態による電子商取引手順
第1の実施の形態においては、購入者が商品の購入の際に、販売元から自宅への商品配達に必要な最低限な氏名及び住所のみを用いることによって私的又は個人的な情報の漏洩を防止する場合について説明したが、以下においては、自宅に換えて例えばコンビニエンスストアという購入者がよく利用する店で商品を受け取ることでより私的な情報の漏洩を防止した電子商取引システムについて説明する。

【0117】図1との対応部分に同一符号を付して示す図4は、第2の実施の形態による電子商取引システム100を示し、個人端末2に換えて、インターネットに接続する購入端末109を設置している例えばコンビニエンスストア（以下、これを公衆インターネットボックス200と呼ぶ）を用いる点を除いて、第1の実施の形態と同様に構成されている。

【0118】ここで図4との対応部分に同一符号を付して示す図5を用いて、第2の実施の形態による電子商取引システム100において、電子小切手を使用して商品の購入を行うその取引状況を説明する。

【0119】実際上、公衆インターネットボックス200個において商品を購入しようとする購入者は、まず自己の指紋照合器8を購入端末109に接続する。

【0120】そして購入端末109は、購入者が自分の指を指紋照合器8の指紋採取部10に載せ、当該指紋照合器8が購入者の指紋に基づいて購入者の正当性を確認

なる。

【0121】続けて購入端末109は、購入者が購入端末109のディスプレイ（図示せず）に表示される商品の電子カタログを見ながら購入を希望する商品を選択すると、その購入商品の合計金額を算出する。

【0122】購入端末109は、購入者が購入端末109を操作して電子小切手発行依頼コマンドを受け取ると、当該購入端末109に接続されている指紋照合器8の各部を制御すると共に、購入を希望する商品の合計金額及び電子カタログに記載された当該商品を扱う販売元の販売元IDを指紋照合器8のCPU15に送出する。

【0123】指紋照合器8のCPU15は、購入端末109から供給された合計金額及び販売元IDを受け取り、これらのハッシュ値（H1）をハッシュ関数に基づいて算出する。

【0124】このとき指紋照合器8のCPU15は、予め作成した個人用公開鍵Ce及び個人用秘密鍵Cdを使用し得るため、この場合に限り、算出したハッシュ値（H1）を個人用秘密鍵でディジタル署名して署名情報〔(H1)^{Cd}〕を作成する（ステップSP3）。

【0125】指紋照合器8は、購入端末109を介して、作成した署名情報〔(H1)^{Cd}〕と、単なる手続き的な情報である合計金額及び販売元IDを、電子小切手依頼書ファイル〔合計金額＋販売元ID＋署名情報（H1）^{Cd}〕（以下、これを電子小切手依頼書と呼ぶ）として電子銀行5側の銀行サーバ6に送出する（ステップSP4）。

【0126】一方銀行サーバ6は、第1の実施の形態のステップSP5～ステップSP7において上述した手順に従って電子小切手を発行し、これを公衆インターネットボックス200の購入端末109に送出する。

【0127】購入端末109は、銀行サーバ6から電子小切手を受け取ると、これを当該購入端末109に接続されている指紋照合器8に送出する。

【0128】指紋照合器8のCPU15は、購入端末109から電子小切手が供給されると、当該電子小切手のハッシュ値（H3）をハッシュ関数に基づいて算出し、これを予め作成している個人用秘密鍵Cdでディジタル署名して署名情報〔(H3)^{Cd}〕を作成する。

【0129】続けて指紋照合器8のCPU15は、購入者が購入端末109のディスプレイに表示される購入画面を用いて購入を希望する発注商品名のみを入力すると、購入端末109を介して商品名及び公衆インターネットボックス200の住所（以下、これを送り先住所と呼ぶ）を受け取る。

【0130】続けて指紋照合器8のCPU15は、電子銀行5側から供給された電子小切手と当該電子小切手に対応する署名情報〔(H3)^{Cd}〕とに加え、かかる商品名及び送り先住所を一組にした発注伝票〔電子小切手＋を販売元3の販売元サーバ4に配送する（ステップSP8）。

【0131】このとき指紋照合器8のCPU15は、所定の情報の暗号化、又はディジタル署名を当該指紋照合器内部で行うことにより、個人用公開鍵Ce及び個人用秘密鍵Cdを不特定多数の購入者が利用する購入端末109に残存させてしまう恐れがなくなる。従って指紋照合器8は、不特定の購入者によるかかる個人用公開鍵Ceの悪用を防止することができる。

【0132】ここで販売元の販売元サーバ4においては、第1の実施の形態のステップSP9～ステップSP10において上述した手順に従って購入者の支払い能力や当該購入者の使用する電子小切手の正当性を確認し、全ての正当性が確認できた後、電子銀行5側から発注商品の代金を受け取る。

【0133】販売元サーバ4は、発注商品の代金を確実に受け取ると、発注伝票の発注商品名に記載された商品を、発注伝票に記載された送り先住所である購入者が指定した公衆インターネットボックス200側に配達する（ステップSP31）。

【0134】一方公衆インターネットボックス200において、購入者は、販売元3側から自分の指定した公衆インターネットボックス200側に商品が届けられると、その届けられた商品を取りに行く（ステップSP32）。かくして購入者は、自分の所望する商品の商品名を販売元に通知するだけで、かかる商品を入手することができる。

【0135】また購入者は、都合のつく時間に公衆インターネットボックス200に商品を取りに行けばよいため、あえて商品の配達を待って自宅に待機するという必要がなくなる。

【0136】（2-2）本実施の形態の動作及び効果
以上の構成において、購入者はインターネットボックス200を用いて電子商取引における商品購入の手続きを行う際、購入を希望する商品名と、商品の配達先としてかかるインターネットボックス200の住所を販売元3に通知する。そして販売元3側は、購入者の希望する商品をかかるインターネットボックス200側に対して配達する。

【0137】従って購入者は、販売元3側に対し商品の送り先をインターネットボックス200側に指定することにより、自分の氏名及び住所を販売元3側に通知する必要がない。これにより販売元3側から購入者の個人情報が洩れなくなる。

【0138】以上の構成によれば、商品の配達先をインターネットボックス200に指定することにより、自分の氏名及び住所を販売元3に通知する必要がなくなる。従って販売元3側から購入者の個人情報が一切洩れなくなる。かくして購入者のプライバシを守ることのできる

【0139】（3）他の実施の形態
なお上述の第1の実施の形態においては、個人端末2のパーソナルコンピュータ9が販売元に発注伝票を送る際、発注商品名、住所及び氏名のデータを暗号化のされていない状態で送出する場合について述べたが、本発明はこれに限らず、かかる発注商品名、住所及び氏名をシンメトリック鍵K（暗号化及び復号化を同一の暗号化鍵で行ういわゆるシンメトリック暗号法で用いる暗号鍵のこと）で暗号化することにより、暗号化情報〔（発注商品名＋住所＋氏名）^{K}〕を作成し、これを販売元に送出するようにしても良い。

【0140】また上述の第1及び第2の実施の形態においては、パーソナルコンピュータ9のディスプレイ又は購入端末のディスプレイに表示される電子カタログを参考にしながら商品を購入する場合について述べたが、本発明はこれに限らず、紙面に印刷された商品カタログの商品名、商品情報、販売元ＩＤ等を参考にして商品を購入しても良い。

【0141】さらに上述の第1の実施の形態においては、ハッシュ値をパーソナルコンピュータ9で算出する場合について述べたが、本発明はこれに限らず、ハッシュ値を指紋照合器2で算出するようにしても良い。

【0142】さらに上述の第2の実施の形態においては、電子小切手を用いて商取引を行う際、商取引で購入する商品の商品名と、商品を配達する配達先の配達先情報と、商品の購入に用いる電子小切手とを用いて商品の発注をインターネットボックス200に設置した購入端末109で行う場合について述べたが、本発明はこれにかぎらず、商品の配達先をインターネットボックス200で使用できる種々の端末（例えば、携帯用のパーソナルコンピュータ、ネットワーク対応の携帯電話器等）で行うようにしても良い。

【0143】さらに上述の第2の実施の形態においては、インターネットボックス200としてコンビニエンスストアを用いる場合について述べたが、本発明はこれに限らず、書店等の購入者がよく利用する商店や、電子商取引を行うために専用に設けたインターネットボックスを用いるようにしても良い。

【0144】さらに上述の第1及び第2の実施の形態においては、電子小切手〔電子銀行証明書＋小切手番号＋合計金額＋（（Ｈ2）^{Bd}）^{Se}〕のうち署名情報（Ｈ2）^{Bd}のみを販売元用公開鍵Ｓｅで暗号化する場合について述べたが、本発明はこれに限らず、署名情報（Ｈ2）^{Bd}に加えて小切手番号及び合計金額を販売元用公開鍵Ｓｅで暗号化するようにしても良い。

【0145】これにより銀行サーバ6は、個人端末2との間のポイントで電子小切手が改竄されているか否かを判断できるだけでなく、電子小切手自体の改竄、特に購入者の現金を管理する小切手番号の改竄を防止できる。

おいては、本、車等の有体物を購入する場合について述べたが、本発明はこれに限らず、プリントサービスや、医療サービス等の無体物であるサービスを発注するようにしても良い。

【0147】
【発明の効果】上述のように本発明によれば、電子商取引システムにおいて、電子商取引における発注者側の要求に応じて、指定された金額の支払いを保証した電子小切手を発行する電子小切手発行手段を設け、発注者側は、電子小切手を用いて電子商取引の決済を行うようにしたことにより、電子商取引の受注者側が電子小切手に基づいて確実に代金を得ることができ、また電子商取引によって発注者側が何を購入したか等の購入情報が受注者側以外に漏洩するのを未然に防止することができ、かくして電子商取引の安全性を向上させながら発注者側のプライバシを確実に保護し得る電子商取引システムを実現できる。

【0148】また上述のように本発明によれば、電子商取引方法において、電子商取引における発注者側の要求に応じて、指定された金額の支払いを保証した電子小切手を発行する第1のステップと、発注者側が電子小切手を電子商取引の受注者側に送出するようにして当該電子商取引の決済を行う第2のステップとを設けるようにしたことにより、電子商取引の受注者側が電子小切手に基づいて確実に代金を得ることができ、また電子商取引によって発注者側が何を購入したか等の購入情報が受注者側以外に漏洩するのを未然に防止することができ、かくして電子商取引の安全性を向上させながら発注者側のプライバシを確実に保護し得る電子商取引方法を実現できる。

【0149】また上述のように本発明によれば、情報処理装置において、電子商取引における発注者側の要求に応じて、指定された金額の支払いを保証した電子小切手を発行する電子小切手発行手段を設けるようにしたことにより、電子商取引の受注者側が電子小切手に基づいて確実に代金を得ることができ、また電子商取引によって発注者側が何を購入したか等の購入情報が受注者側以外に漏洩するのを未然に防止することができ、かくして電子商取引の安全性を向上させながら発注者側のプライバシを確実に保護し得る情報処理装置を実現できる。

【図面の簡単な説明】
【図1】第1の実施の形態による電子商取引システムを示すブロック図である。
【図2】個人端末の構成を示すブロック図である。
【図3】第1の実施の形態による電子商取引システムの説明に供する略線図である。
【図4】第2の実施の形態による電子商取引システムを示すブロック図である。
【図5】第2の実施の形態による電子商取引システムの

【符号の説明】
1、100……電子商取引システム、2……個人端末、3……販売元、4……販売元サーバ、5……電子銀行、6……銀行サーバ、7……インターネット、8……指紋照合器、9……パーソナルコンピュータ、11……照合コントローラ、13……フラッシュROM、15……CPU、27……暗号エンジン、109……購入端末、200……インターネットボックス。

【図1】

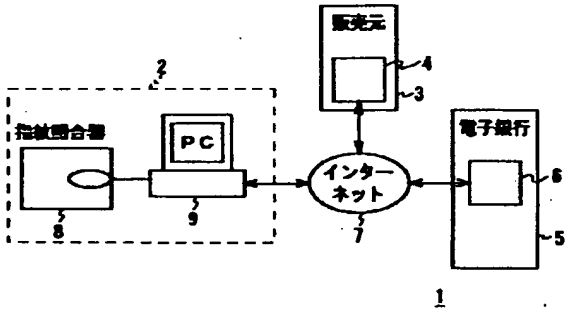

図1　第1の実施の形態による電子商取引システム

【図2】

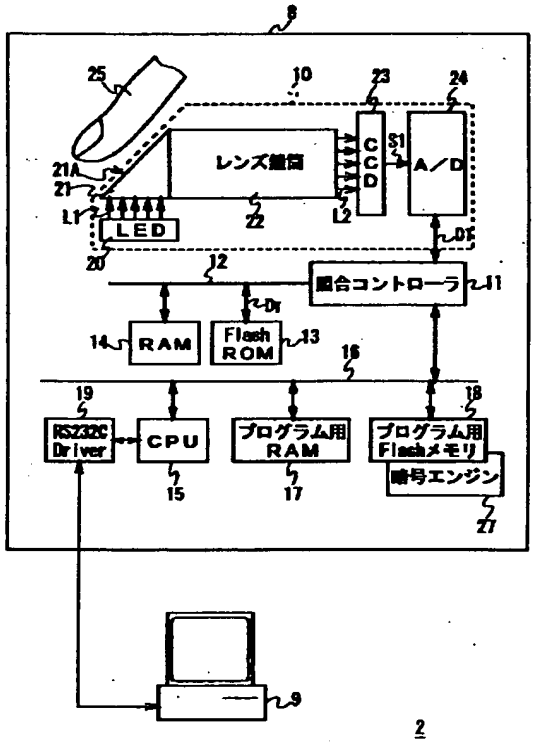

図2　個人端末の構成

【図3】

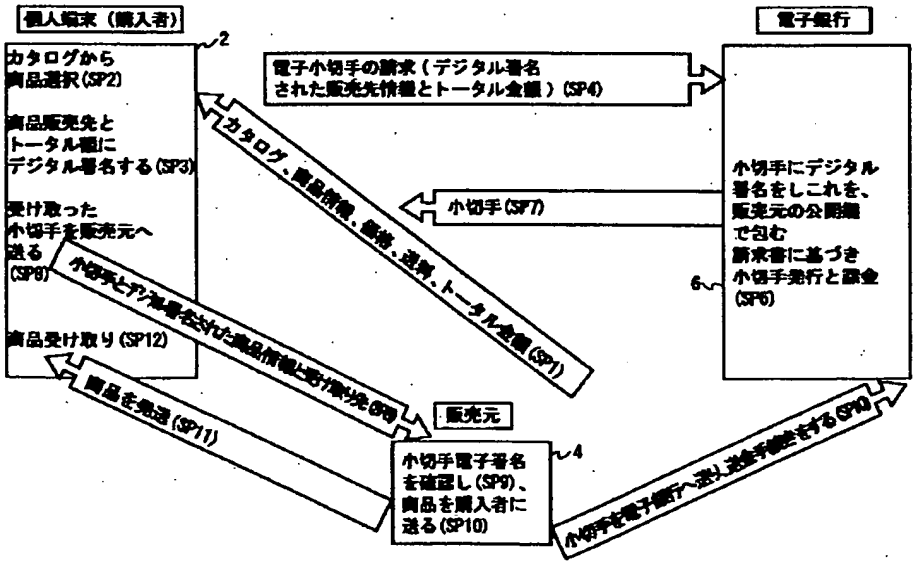

図3　第1の実施の形態による電子商取引システム

【図4】

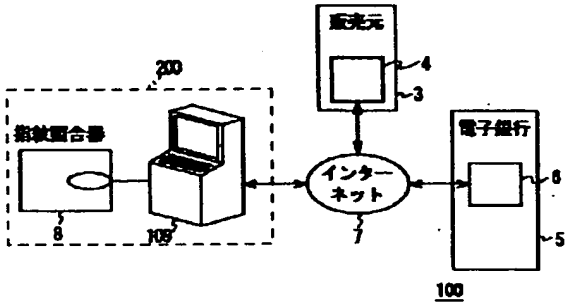

図4　第2の実施の形態による電子商取引システム

【図5】

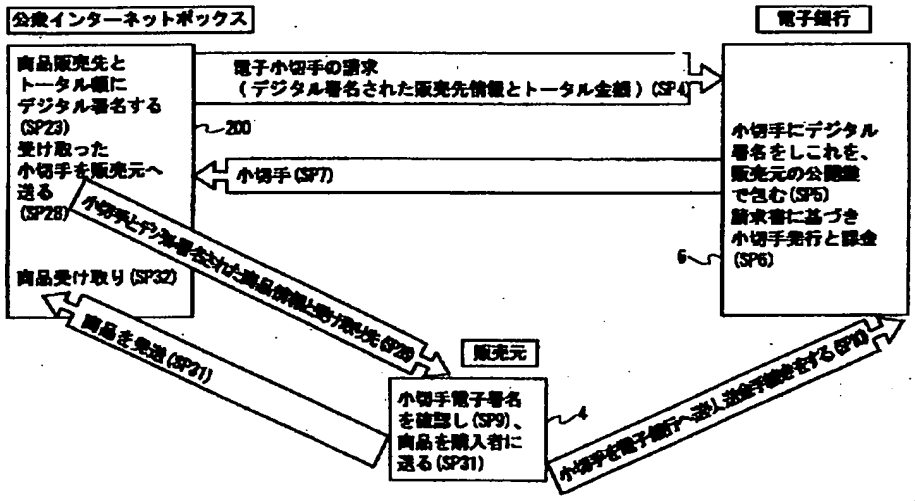

図5　第2の実施の形態による電子商取引システム

フロントページの続き

(51)Int.Cl.[7]		識別記号	FI		テーマコード(参考)
G09C	1/00	660	G09C	1/00	660B
H04L	9/32		H04L	9/00	673D

Fターム(参考)　5B049 AA05 BB11 BB46 CC05 CC36
EE03 EE05 EE09 EE10 FF03
FF04 GG04 GG06 GG07 GG10
5B055 BB12 CC13 EE02 EE03 EE17
EE21 EE27 FA05 FB03 HB02
HB06 JJ05 PA05 PA34
5J104 AA07 AA09 KA01 KA17 LA05
LA06 NA12 PA09 PA10
9A001 JJ64 JJ67 KK58 LL03